

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 11249967
PUBLICATION DATE : 17-09-99

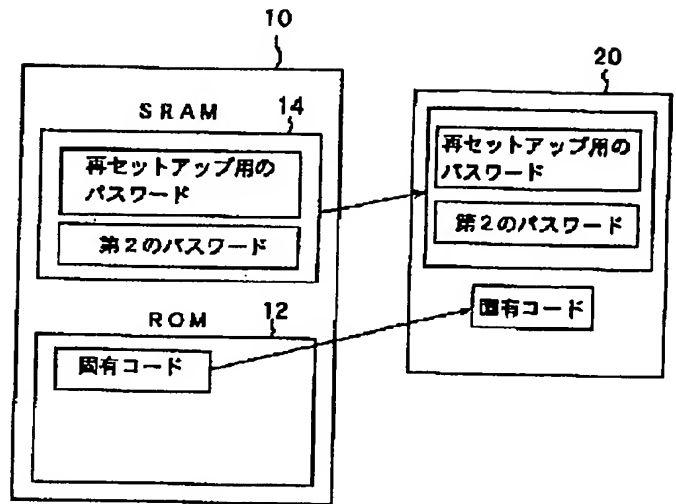
APPLICATION DATE : 27-02-98
APPLICATION NUMBER : 10061888

APPLICANT : FANUC LTD;

INVENTOR : TANOSAKI EIJI;

INT.CL. : G06F 12/14 G06F 12/16

TITLE : METHOD FOR PREVENTING UNJUST
COPY OF NC DATA



ABSTRACT : PROBLEM TO BE SOLVED: To prevent peculiar data set up by an NC maker from being copied and unjustly used and to enable a legal user to smoothly perform the restoration work of a numerical controller.

SOLUTION: When backup data of an SRM 14 is preserved in a memory card 20, a peculiar code of a ROM 12 is written in the memory card 20. When backup information is set up again, it is discriminated whether a peculiar code of a numerical controller 10 is matched with the peculiar code of the memory card 20 or not, and backup information is permitted to be set up again only in the case of coincidence between them, thereby preventing backup data generated in another numerical controller from being unjustly taken in.

COPYRIGHT: (C)1999,JPO

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-249967

(43)公開日 平成11年(1999) 9月17日

(51)Int.Cl.⁸

G 0 6 F 12/14
12/16

識別記号

3 2 0
3 1 0

F I

G 0 6 F 12/14
12/16

3 2 0 F
3 1 0 M

審査請求 未請求 請求項の数3 F D (全 11 頁)

(21)出願番号

特願平10-61888

(22)出願日

平成10年(1998) 2月27日

(71)出願人

390008235

ファナック株式会社

山梨県南都留郡忍野村忍草字古馬場3580番地

(72)発明者

藤林 謙太郎

山梨県南都留郡忍野村忍草字古馬場3580番地 ファナック株式会社内

(72)発明者

菱川 哲夫

山梨県南都留郡忍野村忍草字古馬場3580番地 ファナック株式会社内

(72)発明者

山野崎 英司

山梨県南都留郡忍野村忍草字古馬場3580番地 ファナック株式会社内

(74)代理人

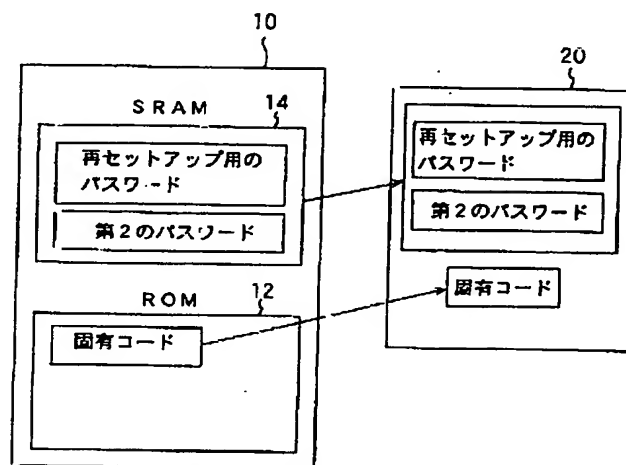
弁理士 竹本 松司 (外4名)

(54)【発明の名称】 NCデータの不正複写防止方法

(57)【要約】

【課題】 NCメーカーでセットアップした固有のデータが複写されて不正利用されるのを防止し、かつ、正当なユーザーによる数値制御装置の復旧作業を円滑化する。

【解決手段】 SRAM14のバックアップデータをメモリカード20に保存する際に、ROM12の固有コードがメモリカード20に書き込まれるようにしておく。バックアップ情報の再セットアップに際しては、その数値制御装置10の固有コードがメモリカード20の固有コードと一致しているか否かを判別し、一致する場合にだけ再セットアップ作業を許容することで、別の数値制御装置で生成されたバックアップデータの不正な持ち込みを禁止する。



【特許請求の範囲】

【請求項1】 数値制御装置に必要とされる不揮発性RAMの情報のバックアップを外部記憶媒体に保存する機能と、前記外部記憶媒体のバックアップ情報を不揮発性RAMに再セットアップする機能とを備えた数値制御装置において、

不揮発性RAMの情報のバックアップを外部記憶媒体に保存する際に、前記数値制御装置に記憶されている書き換え不能な固有コードが強制的に外部記憶媒体に書き込まれるようにしておき、

バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致している場合にだけ再セットアップ作業を実行するようにしたことを特徴とするNCデータの不正複写防止方法。

【請求項2】 再セットアップ用のパスワードが前記固有コードと共に数値制御装置から外部記憶媒体に書き込まれるようにしておき、

バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致していない場合であっても、外部記憶媒体に書き込まれている再セットアップ用のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合には再セットアップ作業を実行するようにしたことを特徴とする請求項1記載のNCデータの不正複写防止方法。

【請求項3】 数値制御装置に記憶されている前記再セットアップ用のパスワードを書き換えるための第2のパスワードを数値制御装置に記憶させておき、数値制御装置に記憶されている第2のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合にだけ前記再セットアップ用のパスワードの書き換えを実行するようにしたことを特徴とする請求項2記載のNCデータの不正複写防止方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、NCデータの不正複写防止方法に関する。

【0002】

【従来の技術】数値制御装置の出荷に際しては、その駆動制御に必要とされるオペレーティングシステムや各種パラメータの値またはアプリケーションプログラム等といった重要な情報を予めNCメーカーがSRAM等の不揮発性RAMに格納して出荷するのが一般的である。

【0003】しかし、実際には、数値制御装置の誤動作や誤った操作、例えば、メモリ保護エラーによる書き込み動作や上書き動作等によって、不揮発性RAM内のオペレーティングシステムや各種パラメータまたはアプリケーションプログラム等のデータに異常や損傷が生じる場合があり、数値制御装置の復旧作業を円滑に行う必要

上、ユーザーサイドで不揮発性RAM内の情報をメモリカード等の外部記憶媒体にバックアップして保存することが多い。

【0004】不揮発性RAMの情報の損傷を生じた数値制御装置、即ち、NCメーカー側で予めオペレーティングシステムや各種パラメータまたはアプリケーションプログラム等をセットアップして出荷した数値制御装置に対してバックアップ情報の再セットアップ作業を行うことで、その数値制御装置を出荷時と同じ状態に戻して使用することには一向に不都合はないが、そのバックアップ情報を別の数値制御装置に移植して利用するのは、契約条件にもよるが、一般に1ライセンス1商品パッケージの原則からは違法であり、そのような不正な複写行為は何らかの方法で禁止する必要がある。

【0005】また、このようなバックアップ情報には非公開のソースコード等が含まれる場合が多いので、バックアップ情報を保存したメモリカード等の外部記憶媒体が第三者の手に渡って複写されると、NCメーカーは機密保持の点で大きな損害を被ることになる。

【0006】

【発明が解決しようとする課題】そこで、本発明の課題は、前記従来技術の欠点を解消し、NCメーカーでセットアップした固有のデータが不用意に複写されて不正に利用されるのを防止し、しかも、正当なユーザーが数値制御装置の復旧作業を円滑に行うことのできるNCデータの不正複写防止方法を提供することにある。

【0007】

【課題を解決するための手段】本発明は、不揮発性RAMの情報のバックアップを外部記憶媒体に保存する際に、数値制御装置に記憶されている書き換え不能な固有コードが強制的に外部記憶媒体に書き込まれるようにしておき、バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致している場合にだけ再セットアップ作業を実行するようにしたことを特徴とする構成により前記課題を達成した。

【0008】従って、ある数値制御装置で生成されたバックアップ情報を固有コードが異なる別の数値制御装置に移植することは事実上不可能となり、また、バックアップ情報を生成した数値制御装置に対して正当なユーザーがバックアップ情報を再セットアップする場合には、固有コードの一致によりシリアルナンバー等の入力を省略して円滑な再セットアップ作業を行うことができる。しかも、バックアップ情報を保存した外部記憶媒体には書き換え不能な固有コードが書き込まれるので、外部記憶媒体の不正な持ち出しや貸与があった場合には、その出所、即ち、そのバックアップ情報を生成した数値制御装置を容易に突き止めることができる。

【0009】また、再セットアップ用のパスワードが前記固有コードと共に数値制御装置から外部記憶媒体に書

き込まれるようにしておき、バックアップ情報の再セットアップに際し、外部記憶媒体に書き込まれている固有コードが数値制御装置の固有コードと一致していない場合であっても、外部記憶媒体に書き込まれている再セットアップ用のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合には再セットアップ作業を実行できるようにすることで、NCメーカーの委託を受けた現地作業員のサービス業務の能率化を図った。

【0010】例えば、新たなライセンス契約を付加することにより、その時点で既にそのユーザーが他の数値制御装置でライセンスを取得して使用していた機能をその時点でユーザーが保有する別の数値制御装置に付加して利用しようとする場合、ライセンス契約を加えようとする数値制御装置に必要とされるバックアップ情報がその場にはない場合でも、NCメーカーの委託を受けて再セットアップ用のパスワードを開示されている現地作業員さえいれば、既存の数値制御装置に他の数値制御装置で生成したバックアップ情報を用いて再セットアップ作業を行うことで数値制御装置に新たな機能を付加することができる。従って、NCメーカーがユーザーから既存の数値制御装置を回収して再セットアップ作業を行う必要はなく、また、ユーザーが保有する既存の数値制御装置の固有コードを調べてその数値制御装置に見合ったバックアップ情報を一々外部記憶媒体に記憶させてユーザーに頒布する必要もなくなり、ライセンスの更新作業を円滑に行うことができる。しかも、ライセンスを更新した数値制御装置で生成されたバックアップ情報を外部記憶媒体に保存する際には、その数値制御装置自体の固有コードが書き込まれることになるので、一旦ライセンスを更新してしまえば、その数値制御装置に異常が発生した場合の再セットアップ作業はユーザー自身の手で簡単に行うことができる。

【0011】更に、数値制御装置に記憶されている再セットアップ用のパスワードを書き換えるための第2のパスワードを数値制御装置に記憶させておき、数値制御装置に記憶されている第2のパスワードと作業者が数値制御装置に入力したパスワードとが一致した場合にだけ再セットアップ用のパスワードの書き換えを実行できるようにしたことで、現地作業員の信頼性の低下に伴うNCメーカー側の危険負担を小さくした。

【0012】NCメーカーのみが知る第2のパスワードを使用して再セットアップ用のパスワードを書き換えれば、その数値制御装置で生成されたバックアップ情報に含まれる再セットアップ用のパスワードと現地作業員が以前に知らされた再セットアップ用のパスワードとが異なるようになるので、その数値制御装置で生成されたバックアップ情報を他の数値制御装置に移植することは現地作業員にもできなくなる。また、第2のパスワードによって再セットアップ用のパスワードの書き換えがプロテクトされるため、何らかの方法で不正な複写作業が行

われた場合でも再セットアップ用のパスワード自体は外部記憶媒体またはそのデータを複写された数値制御装置にそのまま残ることになり、再セットアップ用のパスワードを確認することにより、そのバックアップ情報を生成した数値制御装置や不正な作業を行った現地作業員を容易に突き止めることができる。

【0013】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図1は本発明の不正複写防止方法を適用した一実施形態の数値制御装置10と該数値制御装置10によって駆動制御される工作機械の要部を示すブロック図である。

【0014】プロセッサ11は数値制御装置10を全体的に制御するプロセッサであり、ROM12に格納されたシステムプログラムをバス21を介して読み出し、このシステムプログラムに従って、数値制御装置10を全体的に制御する。RAM13には一時的な計算データ、表示データ等が格納される。

【0015】SRAM14は図示しないバッテリーでバックアップされ、数値制御装置10の電源がオフにされても記憶状態が保持される不揮発性RAMとして構成され、NCメーカーでセットアップしたデータ、例えば、オペレーティングシステムや各種パラメータまたはアプリケーションプログラム等に関連した重要な情報が格納されている。

【0016】インターフェイス15は外部機器用のインターフェイスであり、外部記憶媒体となるメモ리카ード20に対してデータの読み書きを行うためのドライブユニット72が接続され、SRAM14からメモ리카ード20へのデータのバックアップ作業や、メモ리카ード20からSRAM14へのデータの再セットアップ作業が実施できるようになっている。

【0017】SRAM14からメモ리카ード20へのデータのバックアップ作業に必要とされるエンコードや圧縮およびデータ書き出し用のプログラムと、メモ리카ード20からSRAM14へのデータの再セットアップ作業に必要とされる解凍やデコードおよびデータ書き込み用のプログラムは、各々ROM12に格納されている。

【0018】また、装置のシリアルナンバー等で構成される数値制御装置10の固有コードは書き換え不能な状態でROM12に格納され、再セットアップ用のパスワード、および、このパスワードを書き換えるための第2のパスワードの各々は、数値制御装置10の出荷段階で予めNCメーカーによってSRAM14に登録されている。

【0019】このうち装置の出荷段階で最初にSRAM14に登録した再セットアップ用のパスワード、または、その後でNCメーカーが書き換えた再セットアップ用のパスワードの内容に関してはNCメーカーがサービス業務を委託する現地作業員に対して開示するが、再セ

ットアップ用のパスワードを書き換えるための第2のパスワードの情報に関してはNCメーカー内部で秘匿するようにする。

【0020】PMC（プログラマブル・マシン・コントローラ）16は数値制御装置10に内蔵されたシーケンスプログラムで工作機械を制御する。即ち、加工プログラムで指令された機能に従って、これらシーケンスプログラムで工作機械側に必要な信号に変換し、I/Oユニット17から工作機械側へ出力する。この出力信号により工作機械側の各種アクチュエータが作動する。また、工作機械側のリミットスイッチおよび機械操作盤の各種スイッチ等の信号を受けて、必要な処理をしてプロセッサ11に渡す。

【0021】各軸の現在位置、アラーム、画像データ等の信号はCRT/MDIユニット70の表示装置に送られ、表示装置に表示される。インターフェイス18はCRT/MDIユニット70のキーボードからのデータを受けてプロセッサ11に渡す。インターフェイス19は手動パルス発生器71に接続され、手動パルス発生器71からのパルスを受ける。手動パルス発生器71は工作機械側の機械操作盤に実装され、手動で機械可動部を精密に位置決めするために使用される。

【0022】軸制御回路30～32はプロセッサ11からの各軸の移動指令を受けて、各軸の指令をサーボアンプ40～42に出力する。サーボアンプ40～42はこの指令を受けて各軸のサーボモータ50～52を駆動する。X、Y、Z各軸のサーボモータ50～52には位置速度検出用のパルスコードが内蔵されており、このパルスコードからのフィードバック信号が軸制御回路30～32にフィードバックされる。軸制御回路30～32に内蔵されたサーボ制御CPUの各々はこれらのフィードバック信号と前述の移動指令とに基づいて位置ループ、速度ループ、電流ループの各処理を行い、最終的な駆動制御のためのトルク指令を各軸毎に求めて各軸のサーボモータ50～52の位置、速度を制御する。

【0023】スピンドル制御回路60はスピンドル回転指令およびスピンドルのオリエンテーション等の指令を受けて、スピンドルアンプ61にスピンドル速度信号を出力する。スピンドルアンプ61はこのスピンドル速度信号を受けて、スピンドルモータ62を指令された回転速度で回転させる。また、オリエンテーション指令によって所定の位置にスピンドルモータ62の回転位置を位置決めする。

【0024】図2はバックアップ作業時における数値制御装置10の処理の概略を示す概念図である。

【0025】前述した通り、データのバックアップ作業に必要とされるエンコードや圧縮およびデータ書き出し用のプログラムはROM12に格納されており、ドライブレユニット72にメモ리카ード20をセットしてCRT/MDIユニット70からバックアップデータ作成指令

を入力することにより、プロセッサ11が、SRAM14からメモ리카ード20へのデータの書き出し作業と、それに伴うエンコードや圧縮作業を開始する。

【0026】このとき、数値制御装置10の固有コードがROM12から読み出されてメモ리카ード20に保存され、SRAM14に登録されている再セットアップ用のパスワードと第2のパスワードは、SRAM14内のオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等と共にメモ리카ード20に書き出される。

【0027】従って、数値制御装置10の誤動作やアラートを無視したオペレーターの誤操作等によってSRAM14内のオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に損傷が生じた場合には、メモ리카ード20にバックアップデータとして保存されている情報をそのままSRAM14に再セットアップすることで数値制御装置10の障害復旧を行うことができる。

【0028】図3は再セットアップ作業時におけるプロセッサ11の処理動作を示すフローチャートである。

【0029】作業者がCRT/MDIユニット70から再セットアップ指令を入力すると、これを検出したプロセッサ11は、SRAM14をクリアし、ドライブレユニット72にメモ리카ード20をセットする旨のガイダンスメッセージをCRT/MDIユニット70に表示して（ステップa1）、メモ리카ード20の挿入を待つ待機状態に入る（ステップa2）。

【0030】そして、メモ리카ード20が挿入されると、これを検出したプロセッサ11は、メモ리카ード20に保存されているデータのうち数値制御装置の固有コードに関連した部分のデータをメモ리카ード20からRAM13に読み込んで解凍およびデコードに関する処理を実行し、メモ리카ード20に保存されていた数値制御装置の固有コードとROM12に登録されている固有コードとを比較して（ステップa3）、両者が一致しているか否かを判別する（ステップa4）。

【0031】一致している場合には、メモ리카ード20に保存されているバックアップデータがこの数値制御装置10によって生成されたバックアップデータであって、ユーザーによる合法的な再セットアップ作業が行われようとしていることを意味するので、プロセッサ11は、引き続きメモ리카ード20からオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連したデータを読み込んで解凍およびデコードに関する処理を実行し、復元されたデータとメモ리카ード20に登録されている2つのパスワードを数値制御装置10のSRAM14に書き込んで、SRAM14内のデータを損傷発生前の状態に復旧させる（ステップa9）。

【0032】また、メモ리카ード20に保存されていた

数値制御装置の固有コードとROM12に登録されている固有コードとが一致せずにステップa4の判別結果が偽となった場合、プロセッサ11は、更に、再セットアップ用のパスワードを入力する旨のガイダンスメッセージをCRT/MDIユニット70に表示して（ステップa5）、パスワードの入力を待つ待機状態に入る（ステップa6）。

【0033】そして、作業者がCRT/MDIユニット70のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ11は、メモ리카ード20に保存されているデータのうち再セットアップ用のパスワードに関連した部分のデータをメモ리카ード20からRAM13に読み込んで解凍およびデコードに関する処理を実行し、作業者が入力したパスワードとメモ리카ード20に保存されていた再セットアップ用のパスワードとを比較し（ステップa7）、両者が一致しているか否かを判別する（ステップa8）。

【0034】一致している場合には、再セットアップ作業を行おうとしている作業者が再セットアップ用のパスワードを知っていること、即ち、NCメーカーのサービス業務を委託された現地作業員であることを意味するので、プロセッサ11は、引き続きメモ리카ード20からオペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連したデータを読み込んで解凍およびデコードに関する処理を実行し、復元されたデータとメモ리카ード20に登録されている2つのパスワードを数値制御装置10のSRAM14に書き込む（ステップa9）。

【0035】この場合は、メモ리카ード20に保存されていた数値制御装置の固有コードとROM12に登録されている固有コードとが相違しても再セットアップ作業の実施が可能である。従って、メモ리카ード20に保存されているデータは、最初にNCメーカーがその数値制御装置10にセットアップしたものと同一であるとは限らず、オペレーティングシステムや各種パラメータおよびアプリケーションプログラム等に関連した新たな機能がSRAM14に追加される場合がある。

【0036】例えば、既存の数値制御装置10に対し、より新しい他の数値制御装置で生成したバックアップ情報を用いて再セットアップ作業を行うことによって新たな機能を付加するといった場合がある。この作業を実施できるのは、再セットアップ用のパスワードを開示された現地作業員のみであり、このようなサービスを受けるためには、当然、ユーザーとメーカーとの間で新たなライセンス契約の更新が必要となる。

【0037】このようにして異なる固有コードを有するメモ리카ード20から再セットアップ作業を行って新規機能を追加した場合であっても、数値制御装置10のSRAM14からメモ리카ード20にバックアップを保存する際には、その数値制御装置10自体の固有コードが

ROM12からメモ리카ード20に保存されることになるので、もし、後々その数値制御装置10のSRAM14に損傷が生じたような場合には、再セットアップ用のパスワードを知らないユーザーでも、その数値制御装置10からバックアップデータを保存されたメモ리카ード20を用いて再セットアップ作業を行うことで、固有コードの一致によりSRAM14の損傷を簡単に復旧することができる。

【0038】また、再セットアップ用のパスワードを使用して再セットアップ作業を実施した場合、その時に使用されたパスワードの値が再セットアップの対象となった数値制御装置10のSRAM14にそのまま保存されるので、現地作業員が違法な手続きで再セットアップ作業を行ったような場合、例えば、ライセンス契約を更新せずに他の数値制御装置のSRAM14の内容を数値制御装置10に無断複写したような場合、メーカー側は、SRAM14に保存されている再セットアップ用のパスワードを調べることにより、そのパスワードを使用している現地作業員、即ち、違法な複写作業を行った現地作業員を容易に特定することができる。

【0039】また、メモ리카ード20の側にはそのメモ리카ード20にバックアップデータを保存した数値制御装置10の固有コードが保存されるので、メモ리카ード20自体の不正な持ち出しや貸与があった場合にも、その複写元となった数値制御装置10を容易に特定することができる。

【0040】メモ리카ード20に保存されていた再セットアップ用のパスワードと作業者が入力したパスワードとが一致せずにステップa8の判別結果が偽となった場合には、再セットアップ作業を行おうとしている作業者が再セットアップ用のパスワードを知らないこと、つまり、NCメーカーのサービス業務を委託された正規の現地作業員以外の人間によって不正な複写作業が行われようとしていることを意味するので、プロセッサ11は、ステップa9の再セットアップ処理をキャンセルして処理を終了する。

【0041】以上の処理により、ユーザーによるデータの不正複写は未然に防止されるが、再セットアップ用のパスワードを知っている現地作業員によるデータの不正複写までは禁止できない。従って、より厳格な管理を望むのであれば、必要に応じてメーカー側で数値制御装置10を点検し、SRAM14に不正なデータが持ち込まれていないかどうかを確認する必要がある。

【0042】つまり、数値制御装置10のSRAM14に記憶されている再セットアップ用のパスワードが予めメーカーがその数値制御装置10にセットアップしたパスワードと一致していれば、その数値制御装置10においてSRAM14の内容に損傷を生じた経歴が皆無であるか、または、損傷が生じた経歴があったとしてもその損傷を修復するためにその数値制御装置10自体で生成

したバックアップデータをユーザーが再セットアップしたかのどちらかであり、いずれの場合も問題となる点はない。

【0043】一方、数値制御装置10のSRAM14に記憶されている再セットアップ用のパスワードと予めメーカーがその数値制御装置10にセットアップしたパスワードとが一致していなければ、少なくとも、現地作業員が再セットアップ用のパスワードを使用して別の数値制御装置からバックアップデータを持ち込んだことは明らかとなる。そして、これによって追加された新機能に関する部分のライセンス契約がユーザーとメーカーとの間で取り交わされていれば合法的な作業であり、また、ライセンス契約が更新されていなければ非合法的な作業が行われたことを意味する。

【0044】図4は数値制御装置10のSRAM14に記憶されている再セットアップ用のパスワードをメーカー側で確認する場合の処理を示すフローチャートである。

【0045】作業員がCRT/MDIユニット70からパスワード確認指令を入力すると、これを検出したプロセッサ11は、パスワード確認用の画面をCRT/MDIユニット70に表示して(ステップb1)、第2のパスワードを入力する旨のガイダンスメッセージを表示し(ステップb2)、パスワードの入力を待つ待機状態に入る(ステップb3)。なお、パスワード確認指令の入力方法に関してはユーザーおよび現地作業員には開示せず、NCメーカー内部で秘匿するようにする。

【0046】そして、作業員がCRT/MDIユニット70のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ11は、SRAM14に登録されている第2のパスワードを読み込み、作業員が入力したパスワードとSRAM14に登録されている第2のパスワードとを比較して(ステップb4)、両者が一致しているか否かを判別する(ステップb5)。

【0047】一致している場合には、再セットアップ用のパスワードの確認作業を行おうとしている作業員がNCメーカー側の作業員であることを意味するので、プロセッサ11はSRAM14から再セットアップ用のパスワードを読み込んで、その値をCRT/MDIユニット70に表示して作業員に開示する(ステップb6)。

【0048】また、SRAM14に登録されている第2のパスワードと作業員が入力したパスワードとが一致せずにステップb5の判別結果が偽となった場合には、再セットアップ用のパスワードの確認作業を行おうとしている作業員が第2のパスワードを知らないこと、つまり、NCメーカー側の作業員ではないことを意味するので、プロセッサ11は、ステップb6の表示処理をキャンセルして処理を終了する。

【0049】前述したように、ステップB6の処理で表示された再セットアップ用のパスワードが、メーカーが

その数値制御装置10に予めセットアップしておいたパスワードと一致していれば問題はないが、相違している場合には、少なくとも、現地作業員が再セットアップ用のパスワードを使用してその数値制御装置10に別の数値制御装置からバックアップデータを持ち込んだことを意味しているので、メーカー側としては、これによって追加された新機能に関する部分のライセンス契約がユーザーとメーカーとの間で取り交わされているか否かについて調べてみる必要がある。

【0050】当然、正式なライセンス契約が締結されていれば、新機能の追加に使用したバックアップデータを提供したメモリカード20の再セットアップ用パスワードの情報はメーカー側で管理されている筈であるから、両者の比較は可能である。

【0051】ここで正式なライセンス契約が確認されれば問題はないが、確認されない場合には、NCメーカーがサービス業務を委託した現地作業員がメーカー側に無断で違法なデータ複写作業を行ったことを意味する。

【0052】その現地作業員を突き止めるためにはステップb6の処理で表示された再セットアップ用のパスワードの値を確認すればよい。つまり、メーカー側がその再セットアップ用パスワードを開示した現地作業員が違法なデータ複写作業を行った本人である。

【0053】このような問題が発生して現地作業員の信頼性が低下した場合、再セットアップ用のパスワードの値をそのまま現地作業員が利用できるようにしておくとは危険であるから、再セットアップ用のパスワードを更新して従来のパスワードを利用できなくする必要がある。

【0054】図5および図6は再セットアップ用のパスワードを変更するための処理を示すフローチャートである。

【0055】まず、作業員がCRT/MDIユニット70からパスワード変更指令を入力すると、これを検出したプロセッサ11は、パスワード変更用の画面をCRT/MDIユニット70に表示して(ステップc1)、第2のパスワードを入力する旨のガイダンスメッセージを表示し(ステップc2)、パスワードの入力を待つ待機状態に入る(ステップc3)。なお、パスワード変更指令の入力方法に関してはユーザーおよび現地作業員には開示せず、NCメーカー内部で秘匿するようにする。

【0056】そして、作業員がCRT/MDIユニット70のキーボード等を介してパスワードを入力すると、これを検出したプロセッサ11は、SRAM14に登録されている第2のパスワードを読み込み、作業員が入力したパスワードとSRAM14に登録されている第2のパスワードとを比較して(ステップc4)、両者が一致しているか否かを判別する(ステップc5)。

【0057】一致していない場合には、再セットアップ用のパスワードの変更作業を行おうとしている作業員が第2のパスワードを知らないこと、即ち、作業員がNC

メーカー側の作業者ではないことを意味しているので、プロセッサ11は、ステップc6以降の処理をキャンセルして処理を終了する。従って、この場合には再セットアップ用のパスワードの変更作業は実行されない。

【0058】また、ステップc5の判別結果が真となつてNCメーカー側の作業者であることが確認された場合、プロセッサ11は、更に、それまで使用されていた再セットアップ用のパスワード、つまり、問題が生じて信頼性の低下した再セットアップ用のパスワードを入力する旨のガイダンスメッセージをCRT・MD1ユニット70に表示し（ステップc6）、それまで使用されていた再セットアップ用のパスワードの入力を待つ待機状態に入る（ステップc7）。

【0059】そして、作業者がCRT・MD1ユニット70のキーボード等を介して問題となっているパスワードを入力すると、これを検出したプロセッサ11は、SRAM14に記憶されている再セットアップ用のパスワードを読み込み、作業者が入力したパスワードとSRAM14に記憶されている再セットアップ用のパスワードとを比較して（ステップc8）、両者が一致しているか否か、つまり、その数値制御装置10に対しての再セットアップ作業が本当に現時点で問題とされている再セットアップ用のパスワードを用いて実施されたものであるか否かを判別する（ステップc9）。

【0060】問題とされている再セットアップ用のパスワードと数値制御装置10のSRAM14に記憶されている再セットアップ用のパスワードとが一致しない場合には、その数値制御装置10に対する再セットアップ作業が問題のない再セットアップ用のパスワードによって実施されていることを意味するので、その再セットアップ用のパスワードを無意味に書き換えるべきではない。

【0061】従って、ステップc9の判別結果が偽となった場合、プロセッサ11は、ステップc10以降の処理をキャンセルして処理を終了し、再セットアップ用のパスワードの変更作業を実質的に非実行とする。

【0062】ステップc6～ステップc9の処理は、ユーザーが多数の数値制御装置を所有するような場合に、正当に使用されている数値制御装置の再セットアップ用パスワードが不用意に別のパスワードに書き換えられるといった事故を防止するためのものである。

【0063】また、ステップc9の判別結果が真となった場合には、その数値制御装置10に対する再セットアップ作業が現時点で問題とされている再セットアップ用のパスワードによって実施されたことを意味するので、その数値制御装置10から再び重要な情報が持ち出されるのを防止する必要上、その数値制御装置10の再セットアップ用パスワードを変更して、現地作業員がそれまで使用していた再セットアップ用パスワードを無効にする必要がある。

【0064】この場合、プロセッサ11は、新しいパス

ワードを入力する旨のガイダンスメッセージをCRT/MD1ユニット70に表示して（ステップc10）、新しいパスワードの入力を待ち（ステップc11）、作業者が入力した新しいパスワードを一旦記憶してから再び新しいパスワードの入力を要求し（ステップc12）、その入力を確認した後（ステップc13）、1回目に入力されたパスワードと2回目に入力されたパスワードとを比較して（ステップc14）、両者の一致不一致を判別する（ステップc15）。

【0065】そして、1回目に入力されたパスワードと2回目に入力されたパスワードとが一致しない場合には、パスワードを入力する作業者のキーボード等の操作にミスがあったことを意味するので、プロセッサ11は、再び繰り返してステップc10以降の処理を作業者に実行させる。

【0066】この実施形態の場合、入力するパスワードの機密性を保持する必要上、CRT・MD1ユニット70のディスプレイをブラインド表示にした状態でステップc10～ステップc14の新規パスワードの入力処理を実施するようになっており、作業者自身もキーボード等のミスタッチを自ら確認できないので、作業者にパスワードを2回入力させて数値制御装置10側の内部処理でキーボード等の誤操作を検出するようにしているのである。

【0067】そして、1回目に入力されたパスワードと2回目に入力されたパスワードとが一致してステップc15の判別結果が真となると、プロセッサ11は、作業者が意図する通りの再セットアップ用のパスワードが入力されたものと認め、そのパスワードをSRAM14に上書きすることで、それまで使用されていた再セットアップ用のパスワードを無効にし、新たに設定された再セットアップ用のパスワードを有効にする（ステップc16）。

【0068】一旦メーカー側の作業員が再セットアップ用のパスワードを書き換えてしまえば、それまで現地作業員が使用していた再セットアップ用のパスワードは無効となるので、その数値制御装置10で生成したバックアップデータをメモ리카ード20を介して他の数値制御装置に移植することは現地作業員にもできなくなる。

【0069】

【発明の効果】本発明は、バックアップ情報に保存された固有コードと数値制御装置自体の固有コードとを比較して外部記憶媒体からのバックアップ情報の再セットアップの可否を判定するようにしているので、NCメーカーが不揮発性RAMにセットアップした重要な情報がユーザーの手で不用意に他の数値制御装置に複製されて不正に利用されるのを防止することができる。しかも、正当なユーザーがデータに損傷を生じた数値制御装置の復旧作業を行う場合には、バックアップ情報に保存された固有コードと数値制御装置自体の固有コードとの一致に

より面倒なセキュリティチェックを省略して円滑な再セットアップ作業を行うことができる。

【0070】また、バックアップ情報を保存した外部記憶媒体には、そのバックアップ情報を生成した数値制御装置の固有コードが書き込まれるので、外部記憶媒体の不正な持ち出しや貸与があった場合にも、その出所を容易に突き止めることが可能である。

【0071】更に、再セットアップ用のパスワードを利用することにより、外部記憶媒体に書き込まれている固有コードが数値制御装置自体の固有コードと一致していない場合でも再セットアップ作業を実施できるようにしたので、数値制御装置に新機能を追加する場合のライセンス契約の更新等を始めとする現地作業員のサービス業務を能率よく実施することができる。

【0072】更に、メーカーのみが知る第2のパスワードを使用することによって再セットアップ用のパスワードを書き換えることができるので、現地作業員の信頼性に問題が生じたような場合には、それまで使用されていた再セットアップ用のパスワードを無効にして新たな再セットアップ用パスワードを設定することができる。

【0073】また、第2のパスワードによって再セットアップ用のパスワードの書き換えがプロテクトされるため、何らかの方法で不正な複写作業が行われた場合でも、それに使用された再セットアップ用のパスワードが外部記憶媒体またはそのデータを複写された数値制御装置にそのまま残るので、再セットアップに使用されたパスワードを確認することにより、不正な作業を行った現地作業員を容易に突き止めることができる。

【図面の簡単な説明】

【図1】本発明の不正複写防止方法を適用した一実施形態の数値制御装置の要部を示すブロック図である。

【図2】バックアップ作業時における数値制御装置の処理の概略を示す概念図である。

【図3】再セットアップ作業時の処理動作を示すフローチャートである。

【図4】数値制御装置に記憶されている再セットアップ用のパスワードを確認する場合の処理を示すフローチャートである。

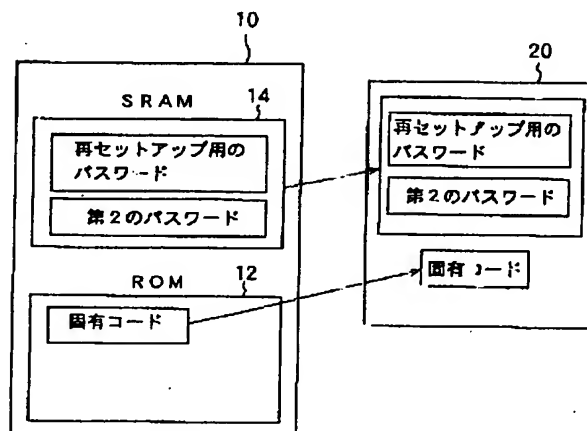
【図5】再セットアップ用のパスワードを変更する場合の処理を示すフローチャートである。

【図6】再セットアップ用のパスワードを変更する場合の処理を示すフローチャートの続きである。

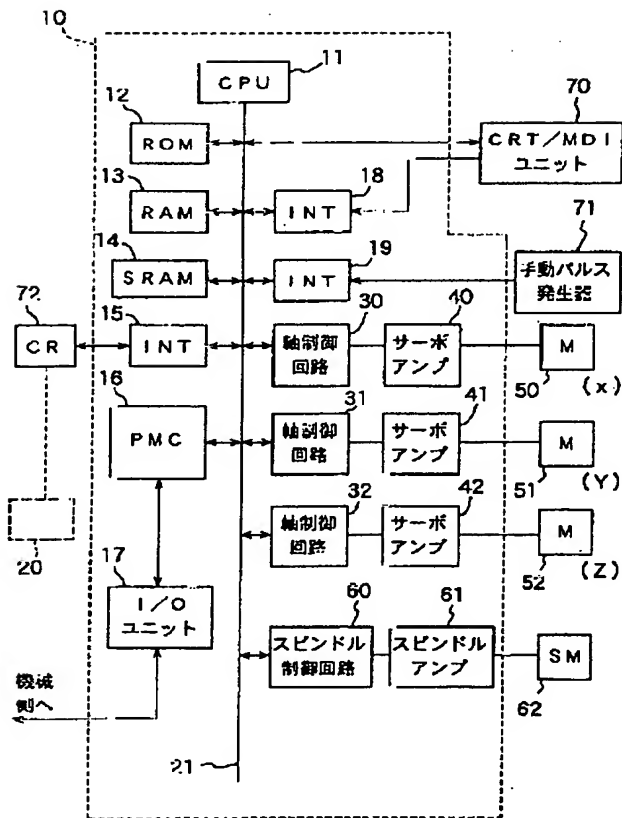
【符号の説明】

- 10 数値制御装置
- 11 プロセッサ
- 12 ROM
- 13 RAM
- 14 SRAM (不揮発性RAM)
- 15 インターフェイス
- 16 PMC (プログラマブル・マシン・コントローラ)
- 17 I/Oユニット
- 18 インターフェイス
- 19 インターフェイス
- 20 メモリカード (外部記憶媒体)
- 21 バス
- 30～32 軸制御回路
- 40～42 サーボアンプ
- 50～52 サーボモータ
- 60 スピンドル制御回路
- 61 スピンドルアンプ
- 62 スピンドルモータ
- 70 CRT/MDIユニット
- 71 手動パルス発生器
- 72 外部記憶媒体のドライブユニット

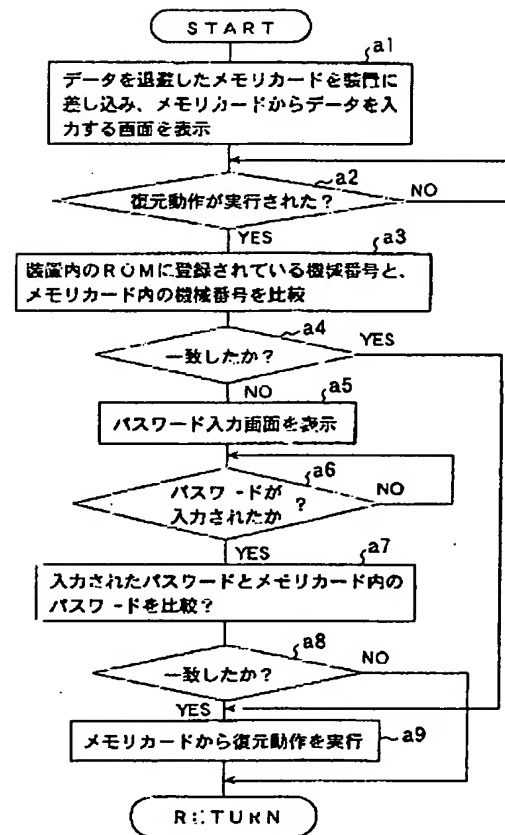
【図2】



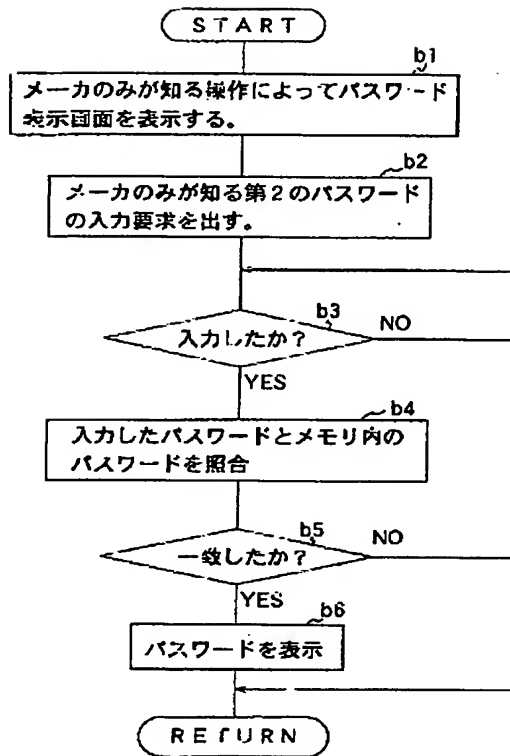
【図1】



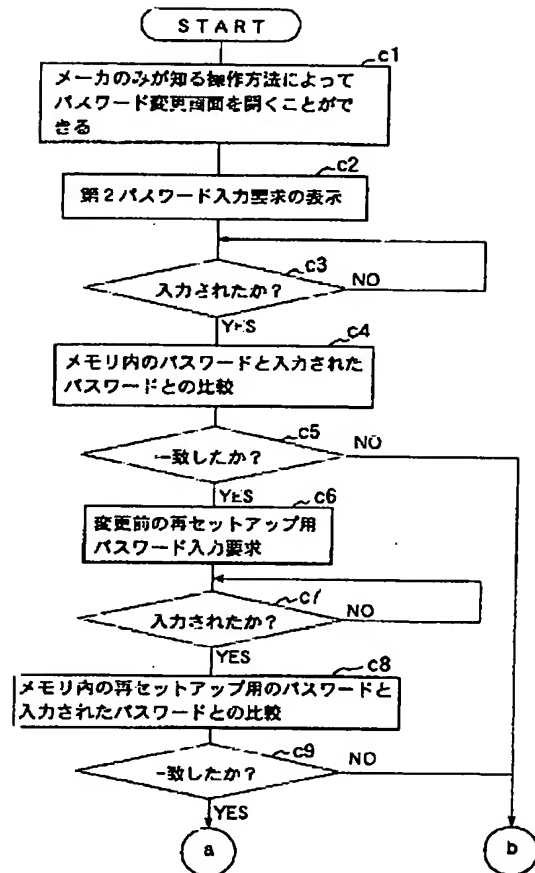
【図3】



【図4】



【図5】



【図6】

